

## **APPENDIX OSS-RESALE & UNE**

**TABLE OF CONTENTS**

**1. INTRODUCTION..... 3**

**2. DEFINITIONS ..... 4**

**3. GENERAL CONDITIONS ..... 4**

**4. PRE-ORDERING..... 7**

**5. ORDERING/PROVISIONING ..... 9**

**6. MAINTENANCE/REPAIR..... 10**

**7. BILLING..... 11**

**8. REMOTE ACCESS FACILITY ..... 12**

**9. DATA CONNECTION SECURITY REQUIREMENTS ..... 13**

**10. .. OPERATIONAL READINESS TEST (ORT) FOR ORDERING/PROVISIONING  
AND REPAIR/ MAINTENANCE INTERFACES ..... 18**

**11. MISCELLANEOUS CHARGES ..... 19**

**12. SERVICE BUREAU PROVIDER ARRANGEMENTS FOR SHARED ACCESS  
TO OSS ..... 19**

**13. APPLICABILITY OF OTHER RATES, TERMS AND CONDITIONS ..... 20**

**APPENDIX OSS  
(ACCESS TO OPERATIONS SUPPORT SYSTEMS FUNCTIONS)**

**1. INTRODUCTION**

- 1.1 This Appendix sets forth terms and conditions for nondiscriminatory access to Operations Support Systems (OSS) “functions” to TWTC for pre-ordering, ordering, provisioning, maintenance/repair, and billing provided by the applicable SBC Communications Inc. (SBC) owned Incumbent Local Exchange Carrier (ILEC). With respect to all matters covered by this Appendix, the Parties will comply with the final SBC-Ameritech POR for Uniform and Enhanced OSS (“Uniform POR”) as approved by FCC on September 22, 2000.
- 1.2 SBC Communications Inc. (SBC) means the holding company which owns the following ILECs: Illinois Bell Telephone Company, Indiana Bell Telephone Company Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Pacific Bell Telephone Company, The Southern New England Telephone Company, Southwestern Bell Telephone Company and/or Wisconsin Bell, Inc. d/b/a Ameritech Wisconsin.
- 1.3 AM-WI - As used herein, AM-WI means the applicable above listed ILEC(s) doing business in Wisconsin.
- 1.4 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.5 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.6 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.7 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.8 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.9 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.10 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.11 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 1.12 AM-WI has established performance measurements to illustrate non-discriminatory access. These measurements are represented in Appendix Performance Measurements.

## 2. DEFINITIONS

- 2.1 “**LSC**” means Information Industry Service Center (IISC) for AM-WI.
- 2.2 “**LOC**” means the Customer Response Unit (CRU) for AM-WI.
- 2.3 “**Service Bureau Provider**” - For purposes of this Agreement, Service Bureau Provider is a company which has been engaged by TWTC to act as its agent for purposes of accessing AM-WI's OSS application-to-application interfaces.

## 3. GENERAL CONDITIONS

- 3.1 Resale and Unbundled Network Elements (UNE) functions will be accessible via electronic interface(s), as described herein, where such functions are available. The Parties agree that electronic order processing is more efficient than manual order processing. During implementation the Parties will negotiate a threshold volume of orders after which electronic ordering is required. Once TWTC is submitting more than the agreed to threshold amount, but not later than twelve (12) months from the Effective Date of this Agreement, TWTC will no longer submit orders manually (and AM-WI shall not be required to accept and process orders manually) except when the electronic order processing is unavailable for a substantial period of time, or where a given order cannot be processed electronically.
- 3.2 **Proper Use of OSS interfaces:**
- 3.2.1 For AM-WI, TWTC agrees to utilize AM-WI electronic interfaces, as described herein, only for the purposes of establishing and maintaining Resale Services or UNEs through AM-WI. In addition, TWTC agrees that such use will comply with AM-WI's Data Connection Security Requirements as identified in Section 9 of this Appendix. Failure to comply with such security guidelines may result in forfeiture of electronic access to OSS functionality. In addition, TWTC shall be responsible for and indemnifies AM-WI against any cost, expense or liability relating to any unauthorized entry or access into, or use or manipulation of AM-WI's OSS from TWTC systems, workstations or terminals or by TWTC employees, agents, or any third party gaining access through information and/or facilities obtained from or utilized by TWTC and shall pay AM-WI for any and all damages caused by such unauthorized entry.
- 3.3 Within AM-WI regions, TWTC's access to pre-order functions described in 4.2.2 and 4.3.2 will only be utilized to view Customer Proprietary Network Information (CPNI) of another carrier's End User where TWTC has obtained an authorization for release of CPNI from the End User and has obtained an authorization to become the End User's Local Service Provider.

- 3.3.1 In AM-WI regions, TWTC must maintain records of individual customers' authorizations for change in local exchange service and release of CPNI which adhere to all requirements of state and federal law, as applicable.
- 3.3.2 **THIS SECTION INTENTIONALLY LEFT BLANK.**
- 3.3.3 Throughout AM-WI region, TWTC is solely responsible for determining whether proper authorization has been obtained and holds AM-WI harmless from any loss on account of TWTC's failure to obtain proper CPNI consent from an End User.
- 3.4 By utilizing electronic interfaces to access OSS functions, TWTC agrees to perform accurate and correct ordering as it relates to Resale and UNE services, rates, and charges, subject to the terms of this Agreement and applicable tariffs dependent on region of operation. TWTC is also responsible for all actions of its employees using any of AM-WI's OSS systems. As such, TWTC agrees to accept and pay all reasonable costs or expenses, including labor costs, incurred by AM-WI caused by any and all inaccurate ordering or usage of the OSS, if such costs are not already recovered through other charges assessed by AM-WI to TWTC. In addition, TWTC agrees to indemnify and hold AM-WI harmless against any claim made by an End User of TWTC or other third parties against AM-WI caused by or related to TWTC's use of any AM-WI OSS.
- 3.5 In the event SBC has good cause to believe that TWTC has used AM-WI OSS in a way that conflicts with this Agreement or Applicable Law, SBC shall give TWTC written notice describing the alleged misuse ("Notice of Misuse"). TWTC shall immediately refrain from the alleged misuse until such time that TWTC responds in writing to SBC's Notice of Misuse, which shall be provided to SBC within twenty (20) days after receipt of the Notice of Misuse. In the event TWTC agrees with SBC's allegation of misuse, TWTC shall refrain from the alleged misuse during the term of this Agreement.
- 3.6 In the event TWTC does not agree that TWTC's use of AM-WI OSS is inconsistent with this Agreement or Applicable Law, then the parties agree to the following steps:
- 3.6.1 If such misuse involves improper access of pre-order applications to obtain CPNI in violation of this Agreement, Applicable Law, or involves a violation of the security guidelines contained herein, or negatively affects another OSS user's ability to use OSS, TWTC shall continue to refrain from using the particular OSS functionality in the manner alleged by SBC to be improper, until TWTC has implemented a mutually agreeable remedy to the alleged misuse.
- 3.6.2 To remedy the misuse for the balance of the agreement, Parties will work together as necessary to mutually determine a permanent resolution for the balance of the term of the agreement.

- 3.7 In order to determine whether TWTC has engaged in the alleged misuse described in the Notice of Misuse, and for good cause shown, SBC shall have the right to conduct an audit of TWTC's use of the AM-WI OSS. Such audit shall be limited to auditing those aspects of TWTC's use of the AM-WI OSS that relate to SBC's allegation of misuse as set forth in the Notice of Misuse. AM-WI shall give ten (10) days advance written notice of its intent to audit TWTC ("Audit Notice") under this Section 3.5, and shall identify the type of information needed for the audit. Such Audit Notice may not precede SBC's Notice of Misuse. Within a reasonable time following the Audit Notice, but no less than fourteen (14) days after the date of the notice (unless otherwise agreed by the Parties), TWTC shall provide AM-WI with access to the requested information in any reasonably requested format, at an appropriate TWTC location, unless otherwise agreed to by the Parties. The audit shall be at AM-WI's expense. All information obtained through such an audit shall be deemed proprietary and/or confidential and subject to confidential treatment without necessity for marking such information confidential. SBC agrees that it shall only use employees or outside parties to conduct the audit who do not have marketing, strategic analysis, competitive assessment or similar responsibilities within SBC, or any SBC affiliate.
- 3.8 In areas where Resale Service and UNE order functions are not available via an electronic interface for the pre-order, ordering and provisioning processes, AM-WI and TWTC will use manual processes. Should AM-WI develop electronic interfaces for these functions for itself, AM-WI will make electronic access available to TWTC within the specific operating region.
- 3.9 The Information Services (I.S.) Call Center for the AM-WI region provides for technical support function of electronic OSS interfaces. TWTC will also provide a single point of contact for technical issues related to the TWTC's electronic interfaces.
- 3.10 AM-WI and TWTC will establish interface contingency plans and disaster recovery plans for the pre-order, ordering and provisioning of Resale services and UNE.
- 3.11 The Parties will follow the final adopted guidelines of 13-STATE Change Management Plan, developed in collaboration with CLECs. This plan may be modified from time to time in accordance with the Change Management principles.
- 3.12 AM-WI will and TWTC may participate in the Order and Billing Forum (OBF) and the Telecommunications Industry Forum (TCIF) to establish and conform to uniform industry guidelines for electronic interfaces for pre-order, ordering, and provisioning. Neither Party waives its rights as participants in such forums or in the implementation of the guidelines. To achieve system functionality as quickly as possible, the Parties acknowledge that AM-WI may deploy interfaces with requirements developed in advance of industry guidelines. Thus, subsequent modifications may be necessary to comply with emerging guidelines. TWTC and AM-WI are individually responsible for evaluating the risk of developing their respective systems in advance of guidelines and agree to support their own system

modifications to comply with new requirements. In addition, AM-WI has the right to define Local Service Request (LSR) Usage requirements according to the General Section 1.0, paragraph 1.4 of the practices in the OBF Local Service Ordering Guidelines (LSOG), which states: "Options described in this practice may not be applicable to individual providers tariffs; therefore, use of either the field or valid entries within the field is based on the providers tariffs/practices."

- 3.13 Due to enhancements and on-going development of access to AM-WI's OSS functions, certain interfaces described in this Appendix may be modified, temporarily unavailable or may be phased out after execution of this Appendix. AM-WI shall provide proper notice of interface phase-out as required by the Change Management process.
- 3.14 TWTC is responsible for obtaining operating system software and hardware to access AM-WI OSS functions as specified in: "Requirements for Access to Southwestern Bell OSS Functions" and "Requirements for Access to Pacific Bell OSS Functions" and "SNET W-CIW in Installation Guide" and "CLEC Hardware/Software Requirements for Access of SBC Uniform OSS Applications", or any other documents or interface requirements subsequently generated by SBC for any of its regions.

#### 4. PRE-ORDERING

- 4.1 AM-WI will provide real time access to pre-order functions to support TWTC ordering of Resale services and UNE. The Parties acknowledge that ordering requirements necessitate the use of current, real time pre-order information to accurately build service orders. The following lists represent pre-order functions that are available to TWTC so that TWTC order requests may be created to comply with AM-WI region-specific ordering requirements.
- 4.2 **Pre-ordering functions for Resale Services include:**
- 4.2.1 **THIS SECTION INTENTIONALLY LEFT BLANK**
- 4.2.2 Access to AM-WI retail or resold CPNI and account information for pre-ordering will include: billing name, service address, billing address, service and feature subscription, directory listing information, long distance carrier identity, and for AM-WI, pending service order activity is included. TWTC agrees that TWTC's representatives will not access the information specified in this subsection until after the End User requests that his or her Local Service Provider be changed to TWTC, and an End User authorization for release of CPNI complies with conditions as described in section 3.3 of this Appendix.
- 4.2.3 A telephone number (if the End User does not have one assigned) with the End User on-line;

- 4.2.4 Service availability dates to the End User (where available);
  - 4.2.5 Information regarding whether dispatch is required;
  - 4.2.6 For AM-WI, Primary Interexchange Carrier (PIC) options for intraLATA toll and interLATA toll; and
  - 4.2.7 Service address verification.
- 4.3 **Pre-ordering functions for UNEs include:**
- 4.3.1 Features available at an End Office for a valid service address (as applicable);
  - 4.3.2 Access to AM-WI retail or resold CPNI and account information for pre-ordering will include: billing name, service address, billing address, service and feature subscription, directory listing information, long distance carrier identity, and, for AM-WI only, pending service order activity. TWTC agrees that TWTC's representatives will not access the information specified in this subsection until after the End User requests that his or her Local Service Provider be changed to TWTC, and an End User authorization for release of CPNI complies with conditions as described in Section 3.3 of this Appendix.
  - 4.3.3 Telephone number assignment (if the End User does not have one assigned) with the End User on-line;
  - 4.3.4 For AM-WI, Primary Interexchange Carrier options for intraLATA toll and interLATA toll;
  - 4.3.5 Service address verification; and
  - 4.3.6 For AM-WI, Channel facility assignment (CFA), network channel (NC), and network channel interface (NCI) data.
  - 4.3.7 Pre-order information specific to DSL capable UNE loops as described in the DSL Appendix of this Agreement.
- 4.4 **Electronic Access to Pre-Order Functions:**
- 4.4.1 **THIS SECTION INTENTIONALLY LEFT BLANK**
  - 4.4.1.1 **THIS SECTION INTENTIONALLY LEFT BLANK**
  - 4.4.1.2 **THIS SECTION INTENTIONALLY LEFT BLANK**
  - 4.4.2 **THIS SECTION INTENTIONALLY LEFT BLANK**

4.4.2.1 **THIS SECTION INTENTIONALLY LEFT BLANK.**

4.4.2.2 **THIS SECTION INTENTIONALLY LEFT BLANK**

4.4.2.3 **THIS SECTION INTENTIONALLY LEFT BLANK**

4.4.2.4 **THIS SECTION INTENTIONALLY LEFT BLANK**

4.4.3 **THIS SECTION INTENTIONALLY LEFT BLANK**

4.4.4 **THIS SECTION INTENTIONALLY LEFT BLANK.**

4.4.5 **AM-WI Resale and UNE Services Pre-Order System Availability: AM-WI** will provide TWTC access to the following system:

4.4.5.1 TCNet and EDI are available for the pre-ordering functions listed in section 4.2.

4.4.6 **THIS SECTION INTENTIONALLY LEFT BLANK**

4.4.6.1 **THIS SECTION INTENTIONALLY LEFT BLANK**

#### 4.5 **Other Pre-order Function Availability:**

4.5.1 Where pre-ordering functions are not available electronically, TWTC will manually request this information from the LSC, dependent on operating region, for inclusion on the service order request.

4.5.2 Upon request, Data Validation Files are available for the purpose of providing requesting CLECs with an alternate method of acquiring that pre-ordering information considered relatively static. For AM-WI, the following information is available via Connect: Direct, CD-ROM and TCNet: Street Address Guide (SAG), Service and Feature Availability by NXX, and PIC/LPIC Codes.

## 5. ORDERING/PROVISIONING

5.1 AM-WI provides access to ordering functions (as measured from the time AM-WI receives accurate service requests from the interface) to support TWTC provisioning of Resale services and UNE via one or more electronic interfaces. To order Resale services and UNEs, TWTC will format the service request to identify what features, services, or elements it wishes AM-WI to provision in accordance with applicable AM-WI ordering requirements. AM-WI will provide TWTC access to one or more of the following systems or interfaces:

5.2 **Resale Service Order Request System Availability:**

5.2.1 **THIS SECTION INTENTIONALLY LEFT BLANK**

5.3 **Resale and UNE Service Order Request Ordering System Availability:**

5.3.1 AM-WI makes available to TWTC an Electronic Data Interchange (EDI) interface for transmission of AM-WI ordering requirements via formats provided on the Local Service Request (LSR) as defined by the OBF and via EDI mapping as defined by TCIF. In ordering and provisioning Resale, TWTC and AM-WI will utilize industry guidelines developed by OBF and TCIF EDI to transmit data based upon AM-WI's Resale ordering requirements, dependent on operating region. In ordering and provisioning UNE, TWTC and AM-WI will utilize industry guidelines developed by OBF and TCIF EDI to transmit data based upon AM-WI's UNE ordering requirements dependent on operating region. In addition, Local Number Portability (LNP) and, where applicable, Interim Number Portability (INP), will be ordered consistent with the OBF LSR and EDI process.

5.3.2 **THIS SECTION INTENTIONALLY LEFT BLANK.**

5.3.3 In ordering and provisioning Unbundled Dedicated Transport and local interconnection trunks, TWTC and AM-WI will utilize industry ASR guidelines developed by OBF based upon SBC ordering requirements.

5.4 **THIS SECTION INTENTIONALLY LEFT BLANK**

5.5 **THIS SECTION INTENTIONALLY LEFT BLANK**

5.6 **Provisioning for Resale Services and UNEs in AM-WI:** AM-WI will provision Resale services and UNE as detailed in TWTC order requests. Access to status on such orders will be provided via the following electronic interfaces:

5.6.1 For EDI ordering, AM-WI provide TWTC, and TWTC shall use, an EDI interface for transferring and receiving orders, FOC, Service Order Completion (SOC), and, as available, other provisioning data and information. AM-WI will provide TWTC with a FOC for each Resale service and UNE request.

6. **MAINTENANCE/REPAIR**

6.1 Two real time electronic interfaces are accessible in each region to place, and check the status of, trouble reports for both Resale services and UNEs. Upon request, TWTC may access these functions via the following methods:

6.1.1 **THIS SECTION INTENTIONALLY LEFT BLANK.**

6.1.2 In AM-WI, Electronic Bonding for Trouble Administration (EBTA-GUI) allows TWTC to perform MLT, issue trouble tickets, view status, and view trouble history on-line.

6.1.3 **THIS SECTION INTENTIONALLY LEFT BLANK.**

6.1.4 In AM-WI, Electronic Bonding Interface (EBI) is an interface that is available for trouble report submission and status updates. EBI conforms to ANSI guidelines T1:227:1995 and T1.228:1995, Electronic Communications Implementation Committee (ECIC) Trouble Report Format Definition (TRFD) Number 1 as defined in ECIC document ECIC/TRA/95-003, and all guidelines referenced within those documents, as mutually agreed upon by TWTC and AM-WI. Functions currently implemented include Enter Trouble, Request Trouble Report Status, Add Trouble Information, Modify Trouble Report Attributes, Trouble Report Attribute Value Change Notification, and Cancel Trouble Report, as explained in 6 and 9 of ANSI T1.228:1995. TWTC and AM-WI will exchange requests over a mutually agreeable X.25-based network.

## 7. BILLING

7.1 AM-WI will bill TWTC for Resold services and UNEs. AM-WI will send associated billing information to TWTC as necessary to allow TWTC to perform billing functions. At minimum AM-WI will provide TWTC billing information in a paper format or via magnetic tape, as agreed to between TWTC and AM-WI.

7.1.1 **THIS SECTION INTENTIONALLY LEFT BLANK.**

7.1.2 For Resale Services in AM-WI, TWTC may elect to receive its bill on CD.

7.2 Electronic access to billing information for Resale services will also be available via the following interfaces:

7.2.1 **THIS SECTION INTENTIONALLY LEFT BLANK.**

7.2.2 **THIS SECTION INTENTIONALLY LEFT BLANK.**

7.2.3 **THIS SECTION INTENTIONALLY LEFT BLANK.**

7.2.4 In AM-WI, TWTC may receive electronically a Daily Usage Extract. On a daily basis, this feed provides information on the usage billed to its accounts for Resale services in the industry standardized EMI format.

7.2.5 TWTC may receive Local Disconnect Report records (via CARE records) that indicate when TWTC's End Users change their Competitive Local

Exchange Carrier. In AM-WI this information is provided via the EDI 836 transaction set.

7.2.6 **THIS SECTION INTENTIONALLY LEFT BLANK.**

7.2.7 In AM-WI, TWTC may receive a mechanized bill via the AM-WI Electronic Billing System (AEBS) transaction set.

7.3 Electronic access to billing information for UNE will also be available via the following interfaces:

7.3.1 AM-WI makes available to CLECs a local bill via the AM-WI Electronic Billing System (AEBS) transaction set.

7.3.2 **THIS SECTION INTENTIONALLY LEFT BLANK**

7.3.3 In AM-WI, TWTC will receive a Daily Usage Extract electronically, on a daily basis, with information on the usage billed to its accounts for UNEs in the industry standardized Exchange Message Interface (EMI) format.

7.3.4 AM-WI, TWTC may receive Local Disconnect Report records (via CARE records) electronically that indicate when TWTC's End Users, utilizing AM-WI, ports, change their Competitive Local Exchange Carrier. In AM-WI, this information is provided via the EDI 836 transaction set.

## 8. REMOTE ACCESS FACILITY

8.1 TWTC must access OSS interfaces via a TWTC Remote Access Facility. The ARAF, located in Chicago, IL, serves AM-WI. Connection to these **Remote Access Facilities** will be established via a "port" either through dial-up or direct connection as described in Section 8.2. TWTC may utilize a port to access AM-WI OSS interfaces to perform the supported functions in any AM-WI where TWTC has executed an Appendix OSS.

8.2 For AM-WI, TWTC may use three types of access: Switched, Private Line, and Frame Relay. For Private Line and Frame Relay "Direct Connections," TWTC shall provide its own router, circuit, and two Channel Service Units/Data Service Units (CSU/DSU). The demarcation point shall be the router interface at the ARAF. Switched Access "Dial-up Connections" require TWTC to provide its own modems and connection to the AM-WI ARAF. TWTC shall pay the cost of the call if Switched Access is used.

8.3 For AM-WI, TWTC shall use TCP/IP to access AM-WI OSS via the ARAF. In addition, each TWTC shall have one valid Internet Protocol (IP) network address per region. TWTC shall maintain a user-id / password unique to each individual for accessing an AM-WI OSS on TWTC's behalf. TWTC shall provide estimates

regarding its volume of transactions, number of concurrent users, desired number of private line or dial-up (switched) connections, and length of a typical session.

- 8.4 For AM-WI, TWTC shall attend and participate in implementation meetings to discuss TWTC ARAF access plans in detail and schedule testing of such connections.

## **9. DATA CONNECTION SECURITY REQUIREMENTS**

- 9.1 TWTC agrees that interconnection of TWTC data facilities with AM-WI data facilities for access to OSS will be in compliance with AM-WI's Competitive Local Exchange Carrier (TWTC) Operations Support System Interconnection Procedures document current at the time of initial connection to a RAF. The following additional terms in this Section 9 govern direct and dial up connections between TWTC and the ARAF.

### **9.2 Joint Security Requirements**

- 9.2.1 Both Parties will maintain accurate and auditable records that monitor user authentication and machine integrity and confidentiality (e.g., password assignment and aging, chronological logs configured, system accounting data, etc.)
- 9.2.2 Both Parties shall maintain accurate and complete records detailing the individual data connections and systems to which they have granted the other Party access or interface privileges. These records will include, but are not limited to, user ID assignment, user request records, system configuration, time limits of user access or system interfaces. These records should be kept until the termination of this Agreement or the termination of the requested access by the identified individual. Either Party may initiate a compliance review of the connection records to verify that only the agreed to connections are in place and that the connection records are accurate.
- 9.2.3 Each Party shall notify the other party immediately, upon termination of employment of an individual user with approved access to the other Party's network.
- 9.2.4 Both Parties shall use an industry standard virus detection software program at all times. The Parties shall immediately advise each other by telephone upon actual knowledge that a virus or other malicious code has been transmitted to the other Party.
- 9.2.5 All physical access to equipment and services required to transmit data will be in secured locations. Verification of authorization will be required for access to all such secured locations. A secured location is where walls and doors are constructed and arranged to serve as barriers and to provide uniform protection for all equipment used in the data connections which are

made as a result of the user's access to either TWTC or AM-WI network. At a minimum, this shall include: access doors equipped with card reader control or an equivalent authentication procedure and/or device, and egress doors which generate a real-time alarm when opened and which are equipped with tamper resistant and panic hardware as required to meet building and safety standards.

- 9.2.6 Both Parties shall maintain accurate and complete records on the card access system or lock and key administration to the rooms housing the equipment utilized to make the connection(s) to the other Party's network. These records will include management of card or key issue, activation or distribution and deactivation.

### 9.3 **Additional Responsibilities of Both Parties**

- 9.3.1 Modem/DSU Maintenance And Use Policy: To the extent the access provided hereunder involves the support and maintenance of TWTC equipment on AM-WI's premises, such maintenance will be provided under the terms of the Competitive Local Exchange Carrier (CLEC) Operations Support System Interconnection Procedures document cited above.
- 9.3.2 Monitoring: Each Party will monitor its own network relating to any user's access to the Party's networks, processing systems, and applications. This information may be collected, retained, and analyzed to identify potential security risks without notice. This information may include, but is not limited to, trace files, statistics, network addresses, and the actual data or screens accessed or transferred.
- 9.3.3 Each Party shall notify the other Party's security organization immediately upon initial discovery of actual or suspected unauthorized access to, misuse of, or other "at risk" conditions regarding the identified data facilities or information. Each Party shall provide a specified point of contact. If either Party suspects unauthorized or inappropriate access, the Parties shall work together to isolate and resolve the problem.
- 9.3.4 In the event that one Party identifies inconsistencies or lapses in the other Party's adherence to the security provisions described herein, or a discrepancy is found, documented, and delivered to the non-complying Party, a corrective action plan to address the identified vulnerabilities must be provided by the non-complying Party within thirty (30) calendar days of the date of the identified inconsistency. The corrective action plan must identify what will be done, the Party accountable/responsible, and the proposed compliance date. The non-complying Party must provide periodic status reports (minimally monthly) to the other Party's security organization on the implementation of the corrective action plan in order to track the work to completion.

9.3.5 In the event there are technological constraints or situations where either Party's corporate security requirements cannot be met, the Parties will institute mutually agreed upon alternative security controls and safeguards to mitigate risks.

9.3.6 All network-related problems will be managed to resolution by the respective organizations, TWTC or AM-WI, as appropriate to the ownership of a failed component. As necessary, TWTC and AM-WI will work together to resolve problems where the responsibility of either Party is not easily identified.

9.4 **Information Security Policies And Guidelines For Access To Computers, Networks and Information By Non-Employee Personnel:**

9.4.1 Information security policies and guidelines are designed to protect the integrity, confidentiality and availability of computer, networks and information resources. Sections 9.5 - 9.11 summarize the general policies and principles for individuals who are not employees of the Party that provides the computer, network or information, but have authorized access to that Party's systems, networks or information. Questions should be referred to TWTC or AM-WI, respectively, as the providers of the computer, network or information in question.

9.4.2 It is each Party's responsibility to notify its employees, contractors and vendors who will have access to the other Party's network, on the proper security responsibilities identified within this Appendix. Adherence to these policies is a requirement for continued access to the other Party's systems, networks or information. Exceptions to the policies must be requested in writing and approved by the other Party's information security organization.

9.5 **General Policies**

9.5.1 Each Party's resources are for approved business purposes only.

9.5.2 Each Party may exercise at any time its right to inspect, record, and/or remove all information contained in its systems, and take appropriate action should unauthorized or improper usage be discovered.

9.5.3 Individuals will only be given access to resources that they are authorized to receive and which they need to perform their job duties. Users must not attempt to access resources for which they are not authorized.

9.5.4 Authorized users must not develop, copy or use any program or code which circumvents or bypasses system security or privilege mechanism or distorts accountability or audit mechanisms.

9.5.5 Actual or suspected unauthorized access events must be reported immediately to each Party's security organization or to an alternate contact

identified by that Party. Each Party shall provide its respective security contact information to the other.

## 9.6 **User Identification**

9.6.1 Access to each Party's corporate resources will be based on identifying and authenticating individual users in order to maintain clear and personal accountability for each user's actions.

9.6.2 User identification shall be accomplished by the assignment of a unique, permanent user id, and each user id shall have an associated identification number for security purposes.

9.6.3 User ids will be revalidated on a monthly basis.

## 9.7 **User Authentication**

9.7.1 Users will usually be authenticated by use of a password. Strong authentication methods (e.g. one-time passwords, digital signatures, etc.) may be required in the future.

9.7.2 Passwords must not be stored in script files.

9.7.3 Passwords must be entered by the user in real time.

9.7.4 Passwords must be at least 6-8 characters in length, not blank or a repeat of the user id; contain at least one letter, and at least one number or special character must be in a position other than the first or last one. This format will ensure that the password is hard to guess. Most systems are capable of being configured to automatically enforce these requirements. Where a system does not mechanically require this format, the users must manually follow the format.

9.7.5 Systems will require users to change their passwords regularly (usually every 31 days).

9.7.6 Systems are to be configured to prevent users from reusing the same password for 6 changes/months.

9.7.7 Personal passwords must not be shared. A user who has shared his password is responsible for any use made of the password.

## 9.8 **Access and Session Control**

9.8.1 Destination restrictions will be enforced at remote access facilities used for access to OSS Interfaces. These connections must be approved by each Party's corporate security organization.

9.8.2 Terminals or other input devices must not be left unattended while they may be used for system access. Upon completion of each work session, terminals or workstations must be properly logged off.

## 9.9 User Authorization

9.9.1 On the destination system, users are granted access to specific resources (e.g. databases, files, transactions, etc.). These permissions will usually be defined for an individual user (or user group) when a user id is approved for access to the system.

## 9.10 Software And Data Integrity

9.10.1 Each Party shall use a comparable degree of care to protect the other Party's software and data from unauthorized access, additions, changes and deletions as it uses to protect its own similar software and data. This may be accomplished by physical security at the work location and by access control software on the workstation.

9.10.2 Untrusted software or data shall be scanned for viruses before use on a Party's corporate facilities that can be accessed through the direct connection or dial up access to OSS interfaces.

9.10.3 Unauthorized use of copyrighted software is prohibited on each Party's corporate systems that can be access through the direct connection or dial up access to OSS Interfaces.

9.10.4 Proprietary software or information (whether electronic or paper) of a Party shall not be given by the other Party to unauthorized individuals. When it is no longer needed, each Party's proprietary software or information shall be returned by the other Party or disposed of securely. Paper copies shall be shredded. Electronic copies shall be overwritten or degaussed.

## 9.11 Monitoring And Audit

9.11.1 To deter unauthorized access events, a warning or no trespassing message will be displayed at the point of initial entry (i.e., network entry or applications with direct entry points). Each Party should have several approved versions of this message. Users should expect to see a warning message similar to this one:

*"This is a (**AM-WI** or TWTC) system restricted to Company official business and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use, or modification being used for criminal prosecution."*

9.11.2 After successful authentication, each session will display the last logon date/time and the number of unsuccessful logon attempts. The user is responsible for reporting discrepancies.

## 10. OPERATIONAL READINESS TEST (ORT) FOR ORDERING/PROVISIONING AND REPAIR/ MAINTENANCE INTERFACES

- 10.1 Prior to live access to interface functionality, the Parties must conduct Operational Readiness Testing (ORT), which will allow for the testing of the systems, interfaces, and processes for the OSS functions. ORT will be completed in conformance with agreed upon processes and implementation dates.
- 10.2 Prior to live system usage, TWTC must complete user education classes for AM-WI-provided interfaces that affect the AM-WI network. Course descriptions for all available classes by region are posted on the CLEC website in the Customer Education section. CLEC Training schedules by region are also available on the CLEC website and are subject to change, with class lengths varying. Classes are train-the-trainer format to enable TWTC to devise its own course work for its own employees. Charges as specified below will apply for each class:

Training Rates	5 day class	4.5 day class	4 day class	3.5 day class	3 day class	2.5 day class	2 day class	1.5 day class	1 day class	1/2 day class
1 to 5 students	\$4,050	\$3,650	\$3,240	\$2,835	\$2,430	\$2,025	\$1,620	\$1,215	\$810	\$405
6 students	\$4,860	\$4,380	\$3,890	\$3,402	\$2,915	\$2,430	\$1,945	\$1,455	\$970	\$490
7 students	\$5,670	\$5,100	\$4,535	\$3,969	\$3,400	\$2,835	\$2,270	\$1,705	\$1,135	\$570
8 students	\$6,480	\$5,830	\$5,185	\$4,536	\$3,890	\$3,240	\$2,590	\$1,950	\$1,300	\$650
9 students	\$7,290	\$6,570	\$5,830	\$5,103	\$4,375	\$3,645	\$2,915	\$2,190	\$1,460	\$730
10 students	\$8,100	\$7,300	\$6,480	\$5,670	\$4,860	\$4,050	\$3,240	\$2,430	\$1,620	\$810
11 students	\$8,910	\$8,030	\$7,130	\$6,237	\$5,345	\$4,455	\$3,565	\$2,670	\$1,780	\$890
12 students	\$9,720	\$8,760	\$7,780	\$6,804	\$5,830	\$4,860	\$3,890	\$2,920	\$1,945	\$970

- 10.3 A separate agreement will be required as a commitment to pay for a specific number of TWTC students in each class. TWTC agrees that charges will be billed by AM-WI and TWTC payment is due thirty (30) days following the bill date. TWTC agrees that personnel from other competitive Local Service Providers may be scheduled into any class to fill any seats for which TWTC has not contracted. Class availability is first-come, first served with priority given to CLECs who have not yet attended the specific class.
- 10.4 Class dates will be based upon AM-WI availability and will be coordinated among TWTC, TWTC's AM-WI Account Manager, and SBC Industry Markets CLEC Training Product Management.
- 10.5 TWTC agrees to pay the cancellation fee of the full price noted in the separate agreement if TWTC cancels scheduled classes less than two (2) weeks prior to the scheduled start date. TWTC agrees to provide to AM-WI completed registration forms for each student no later than one week prior to the scheduled training class.

- 10.6 TWTC agrees that TWTC personnel attending classes are to utilize only training databases and training presented to them in class. Attempts to access any other AM-WI system are strictly prohibited.
- 10.7 TWTC further agrees that training material, manuals and instructor guides can be duplicated only for internal use for the purpose of training employees to utilize the capabilities of AM-WI's OSS in accordance with this Appendix and shall be deemed "Proprietary Information" and subject to the terms, conditions and limitations of Section 20 of the General Terms and Conditions.

## 11. MISCELLANEOUS CHARGES

- 11.1 For AM-WI, should TWTC request custom development of an exclusive interface to support OSS functions, such development will be considered by AM-WI on an Individual Case Basis (ICB) and priced as such.

## 12. SERVICE BUREAU PROVIDER ARRANGEMENTS FOR SHARED ACCESS TO OSS

- 12.1 AM-WI shall allow TWTC to access its OSS via a Service Bureau Provider under the following terms and conditions:
- 12.2 Notwithstanding any language in this Agreement regarding access to OSS to the contrary, TWTC shall be permitted to access AM-WI OSS via a Service Bureau Provider as follows:
- 12.2.1 TWTC shall be permitted to access AM-WI application-to-application OSS interfaces, via a Service Bureau Provider where TWTC has entered into an agency relationship with such Service Bureau Provider, and the Service Bureau Provider has executed an Agreement with AM-WI to Allow Service Bureau Provider to establish access to and use of AM-WI's OSS.
- 12.2.2 TWTC's use of a Service Bureau Provider shall not relieve TWTC of the obligation to abide by all terms and conditions of this Agreement. TWTC must ensure that its agent properly performs all OSS obligations of TWTC under this Agreement, which TWTC delegates to Service Bureau Provider.
- 12.2.3 It shall be the obligation of TWTC to provide notice in accordance with the notice provisions of the Terms and Conditions of this Agreement whenever it established an agency relationship with a Service Bureau Provider or terminates such a relationship. AM-WI shall have a reasonable transition time to establish a connection to a Service Bureau Provider once TWTC provides notice. Additionally, AM-WI shall have a reasonable transition period to terminate any such connection after notice from TWTC that it has terminated its agency relationship with a Service Bureau Provider.

- 12.3 Notwithstanding any language in this Agreement regarding Performance Measures to the contrary, AM-WI shall not be obligated to pay liquidated damages or assessments for noncompliance with a performance measurement to the extent that such noncompliance was the result of actions or events beyond AM-WI's control associated with third-party systems or equipment including systems, equipment and services provided by a Service Bureau Provider (acting as TWTC's agent for connection to AM-WI's OSS) which could not be avoided by AM-WI through the exercise of reasonable diligence or delays or other problems resulting from actions of a Service Bureau Provider, including Service Bureau provided processes, services, systems or connectivity.

### **13. APPLICABILITY OF OTHER RATES, TERMS AND CONDITIONS**

- 13.1 Every interconnection, service and network element provided hereunder, shall be subject to all rates, terms and conditions contained in this Agreement which are legitimately related to such interconnection, service or network element. Without limiting the general applicability of the foregoing, the following terms and conditions of the General Terms and Conditions are specifically agreed by the Parties to be legitimately related to, and to be applicable to, each interconnection, service and network element provided hereunder: definitions, interpretation, construction and severability; notice of changes; general responsibilities of the Parties; effective date, term and termination; fraud; deposits; billing and payment of charges; non-payment and procedures for disconnection; dispute resolution; audits; disclaimer of representations and warranties; limitation of liability; indemnification; remedies; intellectual property; publicity and use of trademarks or service marks; no license; confidentiality; intervening law; governing law; regulatory approval; changes in End User local exchange service provider selection; compliance and certification; law enforcement; no third party beneficiaries; disclaimer of agency; relationship of the Parties/independent contractor; subcontracting; assignment; responsibility for environmental contamination; force majeure; taxes; non-waiver; network maintenance and management; signaling; transmission of traffic to third parties; customer inquiries; expenses; conflicts of interest; survival; scope of agreement; amendments and modifications; and entire agreement.